On Rekey Policies for Secure Group Applications

Qingyu Zhang and Ken Calvert
Lab for Advanced Networking
University of Kentucky

http://protocols.netlab.uky.edu/~calvert/private/icccn03-submit.pdf

Motivation

- Rekey policy: when to change the traffic key?
  - Forward/backward secrecy
    - Every membership change
  - Because of resource limitations:
    - Batch-oriented (every *k* membership changes)
    - Periodic (every *T* seconds)
- Note: resources are *rate*-limited
  - Given capacity (of GCKS), can determine min rekey interval
  - Given min/max rekey interval, can determine resources required
- But what do we give up by postponing rekeying?
  - Goal of our work: quantify the tradeoffs so different policies can be compared

Exposure-oriented rekeying

- Basic idea: account for information accessible but not authorized
  - Assumption: information has value, members pay for access
- Exposure at time t: $E(t) = S\, d(t) \cdot x(t)$
  - d(t): number of departed members (since last rekey) at time t
  - x(t): information rate of the source over period containing t
  - Summation is over periods since last rekey
  - E(t) is the amount of information available to departed members (similarly for joined members or both)
- Exposure-oriented rekeying
  - GCKS keeps track of exposure
  - Needs to know d(t), x(t) = rate of transmission of source
  - Rekey when the exposure reaches a threshold

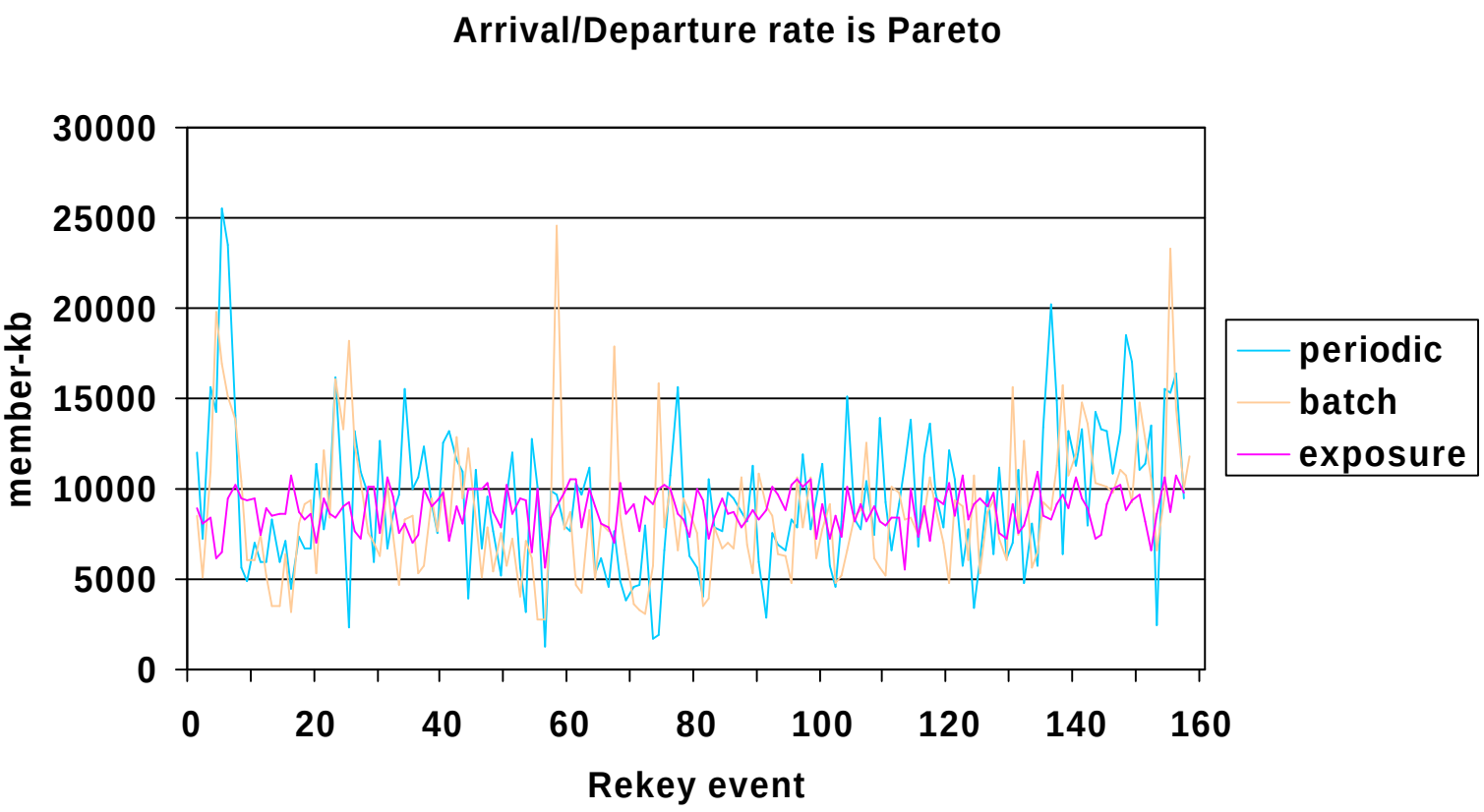
Simulation Setup

- System consists of a GCKS, a sender, and a member simulator
  - Data: MPEG movie; sender reports data rate to GCKS once/sec
  - Interarrival times of requests follows Poisson or Pareto distribution; Join/Leave ratio is 1:1
  - GCKS estimates the exposure whenever it receives a member request, calculates the actual exposure when it gets sender's report (periodically)
  - Group size 500-1000 members; LKH is used as rekey algorithm
- Metrics:
  - Exposure at each rekey event
  - Exposure cost: encryptions/exposed bit
  - Encryption rate: encryptions/time between rekey events

Results – Exposure

Exposure at each rekey event

(Note: events occur at different times)



Results – Exposure (cont'd)

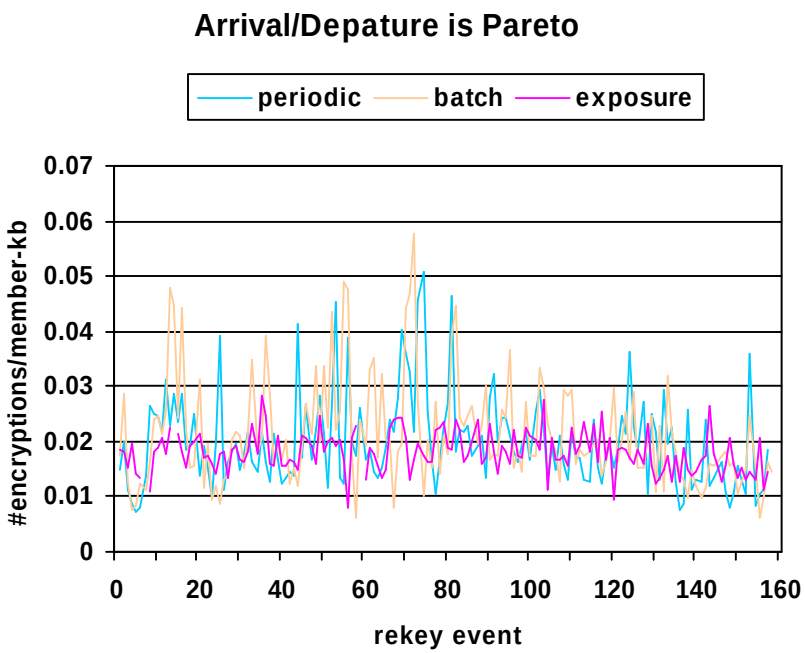
- Standard deviations

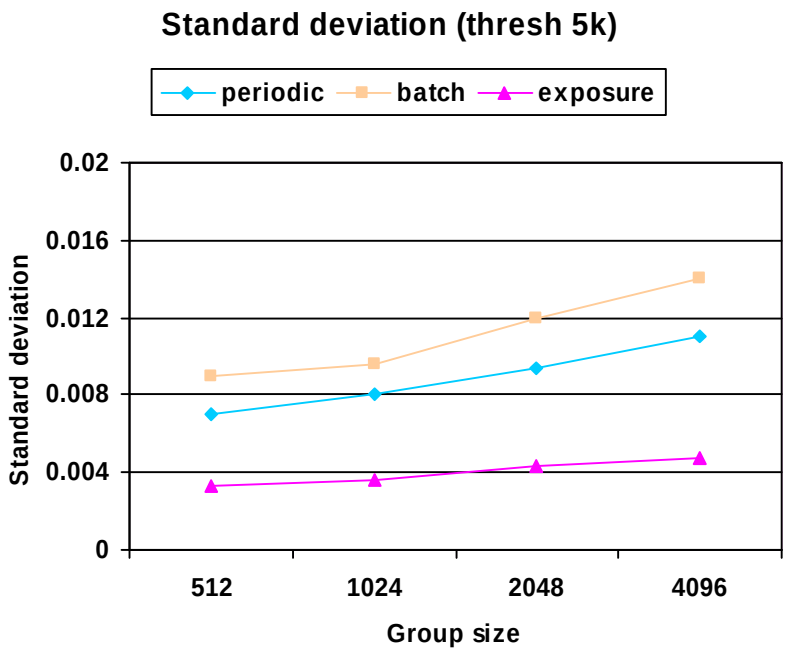
	Exposure			Periodic			Batch		
	2k	5k	13k	7s	12s	19s	16	25	40
Poisson	477	1006	2273	1317	3162	7304	1340	3080	7594
Pareto	519	1091	2318	1775	3911	9336	1629	3846	8625

- Conclusion 1: membership dynamics and information rate affect the exposure; the more variation in either inter-arrival rate or information rate, the more variation in exposure

Results – Exposure Cost Ratio

Encryptions/exposed bit (threshold = 5000 member-kb)

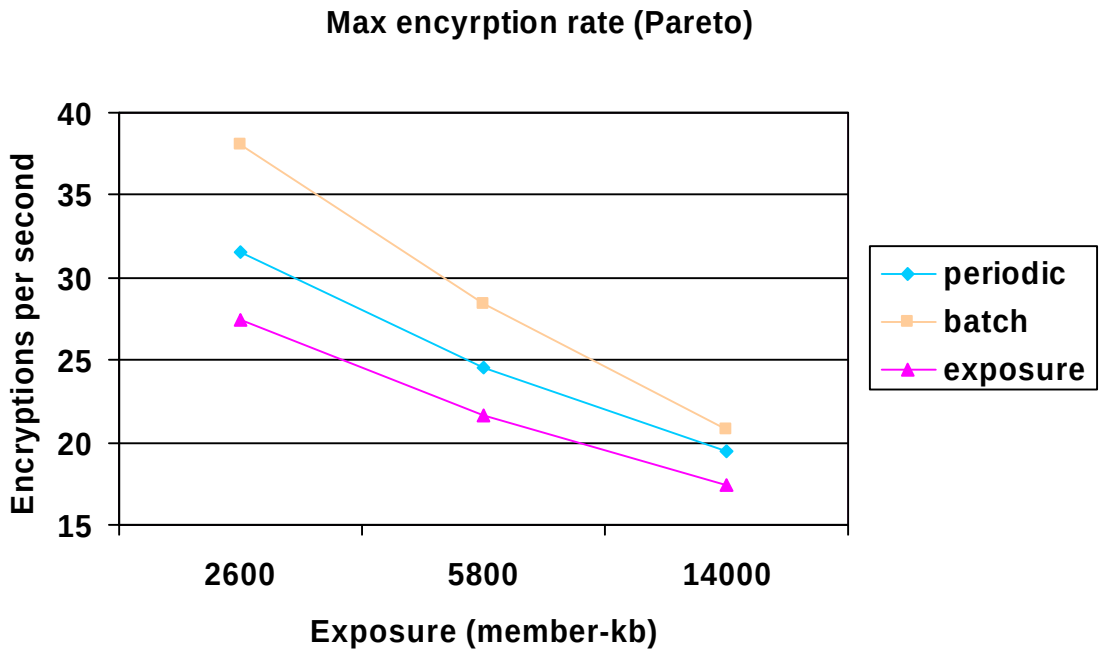




- Conclusion 2: exposure-oriented rekeying balances exposure cost and gives a tighter bound

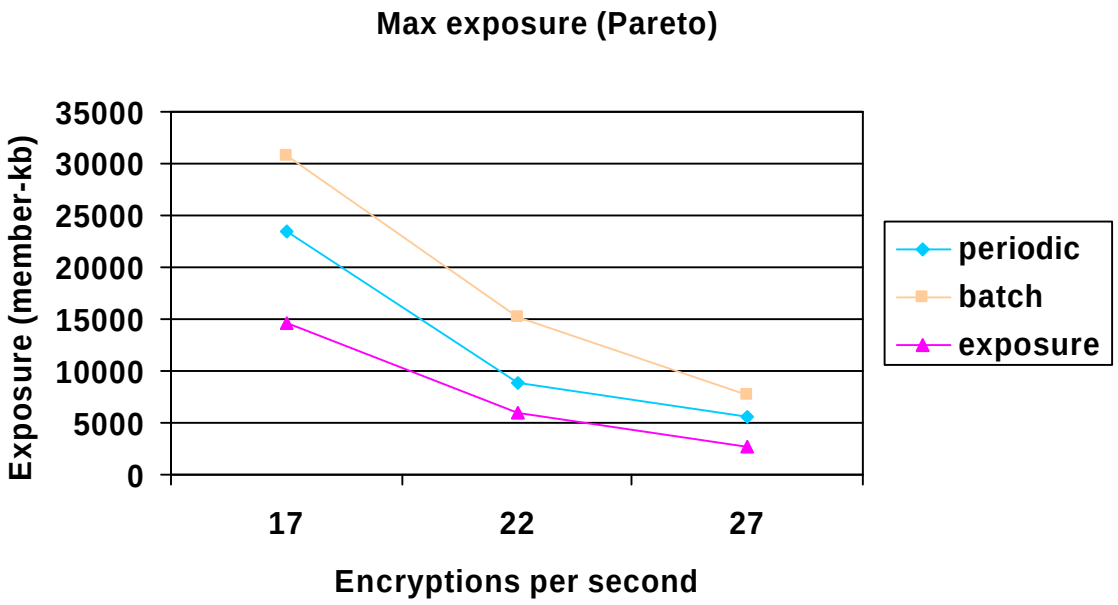
Result – Max Encryption Rate

- Max encryption rate at given max exposure
  - The batch size and rekey interval are adjusted to achieve the same max exposure as exposure-oriented rekeying



Result – Max Encryption Rate

- Max exposure for a given max encryption rate



- Conclusion 3: at given exposure, exposure-oriented rekeying always requires smallest max encryption rate

Summary

- Relaxed rekey policies
  - Amortize cost of rekeying over longer time or multiple membership changes
  - Exposure quantifies the resulting reduction in security
- Exposure-oriented rekeying
  - Quantifies deviation from forward/backward secrecy
  - Performs better in term of peak encryption rate and variation of encryption rate (required to achieve a required level of security)
- Does this belong anywhere in gsec/msec?